Realizing Remote ID

NOVEMBER 2019

Hidden Level, Inc
1153 W Fayette Street
Suite 209
Syracuse, NY 13204

info@hiddenlevel.com

Hidden Level

Table of Contents

DEFINITIONS

ADS-B: Automatic Dependent Surveillance-Broadcast
AGL: Above Ground Level
BVLOS: Beyond Visual Line of Sight
COTS: Commercial Off The Shelf
DAA: Detect and Avoid
GA: General Aviation
IMU: Intertial Measurement Unit
INU: Inertial Navigation Unit
ISM: Industrial, Scientific, and Medical
MOPS: Minimum Operational Performance Standards
SWaP: Size, Weight, and Power
UTM: UAS Traffic Management

Abstract

The FAA UAS integration strategy has evolved rapidly in the last few years with respect to both airspace management and regulatory activities to address the growing needs of present and future airspace users.[1] With industry clamoring to take full advantage of UAS operations, it is clear that Remote Identification (a.k.a. Remote ID) is a critical component to the safe integration of UAS into the airspace. Following on the heels of the Low Altitude Authorization and Notification Capability (LAANC)[2], Remote ID is meant to address the next step in UAS Traffic Management (UTM); the real time identification and location of actively flying UAS. This combined "electronic license plate" and tracking information is needed by public safety personnel and citizens to ensure the fair, safe, and secure use of our airspace and to enable the next wave of UAS applications.

There are several technologies that may provide Remote ID for UAS[3] today and for the near term. This white paper will detail the background of how we got to this point and what the present Remote ID solution trade space looks like. We will then explore some of the long term gaps in Remote ID: non-cooperative UAS, position validation, data security, Beyond Visual Line of Sight (BVLOS), cockpit awareness, and coverage and flexibility. We will propose some potential long term solutions addressing these gaps. Lastly we will discuss how to rapidly move forward and fully realize Remote ID through testing and data collection to inform the final performance-based requirements needed for safe UAS integration.

Remote ID Background

The "drone explosion" that has occurred since 2013 is now old news[36][37]. Both governments and industry alike were not ready to deal with the large influx of consumer drones flooding the skies. Additionally, innovation in the UAS space had driven costs down and the number of use cases were skyrocketing, especially in the commercial markets where UAS were enabling new, low cost operations that replace older, more expensive and risky manned operations.[6]

Late 2015, the FAA mandated registration of all UAS in the US as a stop gap measure.[4] They needed to gather information on exactly how many operators were using the skies[5]; the registration effort proved the point that large scale personal drones were a new reality. There were several attempts at educating the tens of thousands of new pilots by vendors such as DJI[7] and the FAA's Know Before You Fly campaign.[8] The immediate goal was to make information easily accessible on why and how to fly responsibly to promote safety.

At the same time, under the direction of the FAA, NASA was working quickly to find a practical way to integrate these smaller drones into the national airspace. They had launched their UAS Traffic Management (UTM) effort the year prior[9] and brought industry to the table to develop and test ways of interfacing to existing Air Traffic Management (ATM) without further encumbering air traffic controllers. Meanwhile, the tight restrictions on UAS operations remained in effect, culminating in the mid 2016 rollout of 14 CFR Part 107[10], requiring many commercial pilots to apply for waivers to conduct their operations.[11]

The FAA could not keep up with demand for waivers and so the first step was taken to try and ease the waiver application and approval process for commercial flights. The Low Altitude Authorization and Notification Capability (LAANC) system was born[12] and was the first major step in marrying the regulated and unregulated airspace for UTM. While LAANC had immediate benefit to commercial UAV operations, it did almost nothing to address the still growing issue of recreational operators in the airspace - demonstrated abroad with the Gatwick Airport issue in 2018[19]. There was a need for ubiquitous, real time airspace awareness for low altitude UAS flights before the industry could really progress.

Remote ID Background *Cont.*

In 2017 the FAA chartered the UAS Identification and Tracking Aviation Rulemaking Committee (ARC) to provide recommendations for remote identification of drones. There were three objectives[3]:

1. Survey existing and emerging technology that could address Remote ID
2. Identify requirements for meeting security and public safety needs
3. Evaluate the feasibility and affordability of the technical solutions

The final report was delivered later that year and was met with a wide mix of reactions. This paper will not be debate the various points of contention; several excellent white papers have been written supporting many of these different facets[13][14][15].

There have been many proposed Remote ID solutions and while some have certain strengths over others, none resolve material gaps. In order to reap the long term benefits of Remote ID, these gaps must be addressed.

PROPOSED REMOTE ID SOLUTIONS

Section 5.1.1 of the ARC final report grouped the Remote ID technology into eight sub categories and two major categories as presented in the following table[3]:

MAJOR CATEGORY	SUB CATEGORY	DESCRIPTION
Networked	Cellular (CELL)	Existing cell networked in licensed bands.
	Satellite (SAT)	Existing satellite services.
	SW-Based Flight Notification (SWFN)	Uses network connected systems where each UAS/GCS works locally then sends information over the internet.
Direct Broadcast	ADS-B	Automatic Dependent Surveillance-Broadcast. Two variants (1) standard, (2) low power.
	Low Power Direct RF (LPRF)	Variety of protocols in unlicensed spectrum including Bluetooth, Wi-Fi, RFID, etc.
	Unlicensed Integrated C2 (UIC2)	Modulates information onto existing C2 in unlicensed spectrum.
	Physical Indicator (PHYS)	Etched numbers, streamers, etc. Note this may not provide "remote" ID.
	Visual Light Encoding (VLE)	SW controlled LEDs to encode info with specially designed decoders.

While there are other ways to group some of these technologies, especially the ones that could be considered hybrids (e.g. SW based flight notification), two major categories denote the major differences. The solution either has:

NETWORKED

Display device gets the UAS Remote ID relayed over a connected network, for consumption by end user

— OR —

DIRECT BROADCAST

A nearly direct path from the UAS to a receiver/display device to show the UAS Remote ID to the end user

Networked Cellular Architecture

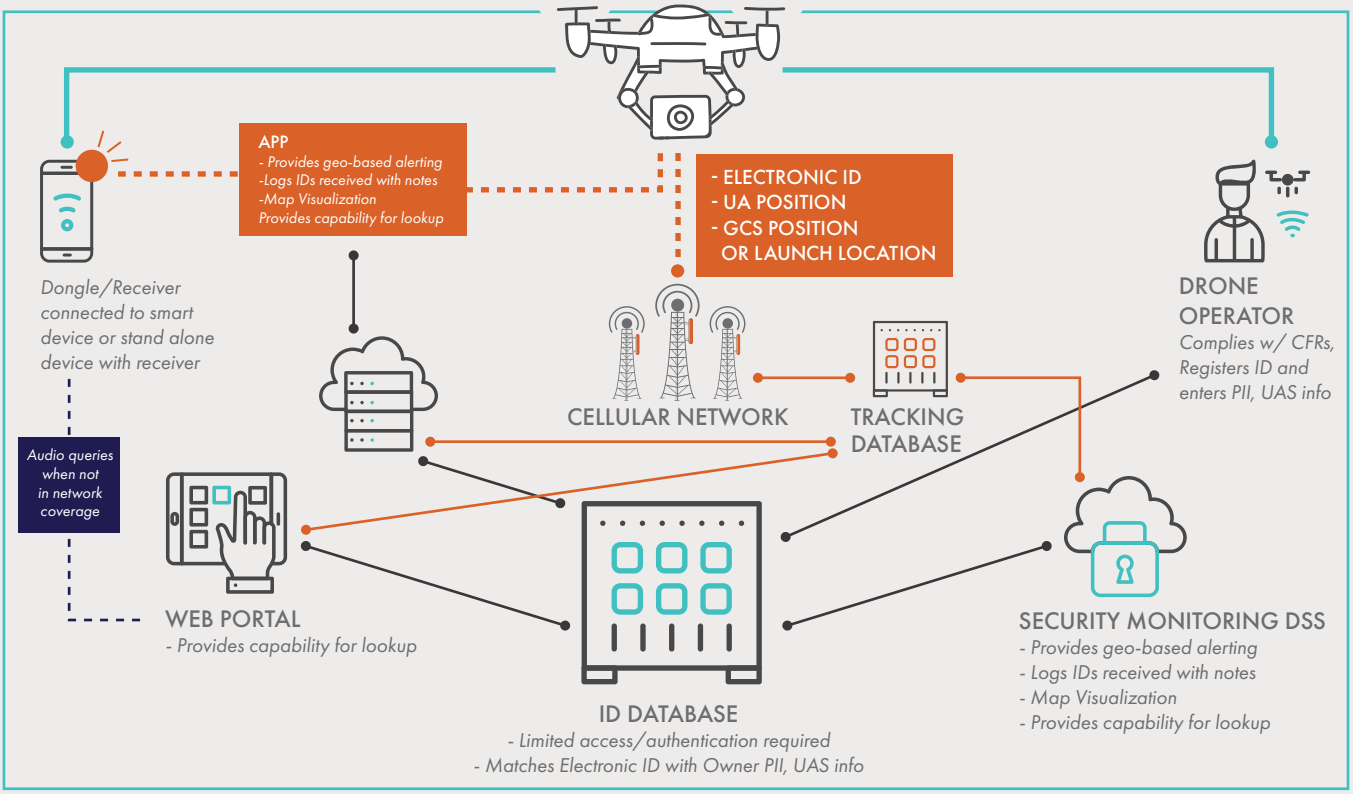


Figure 1. Networked cellular high-level architecture. (Recreation of 2017 FAA UAS ID ARC Report diagram [3])

Low-Power RF Architecture

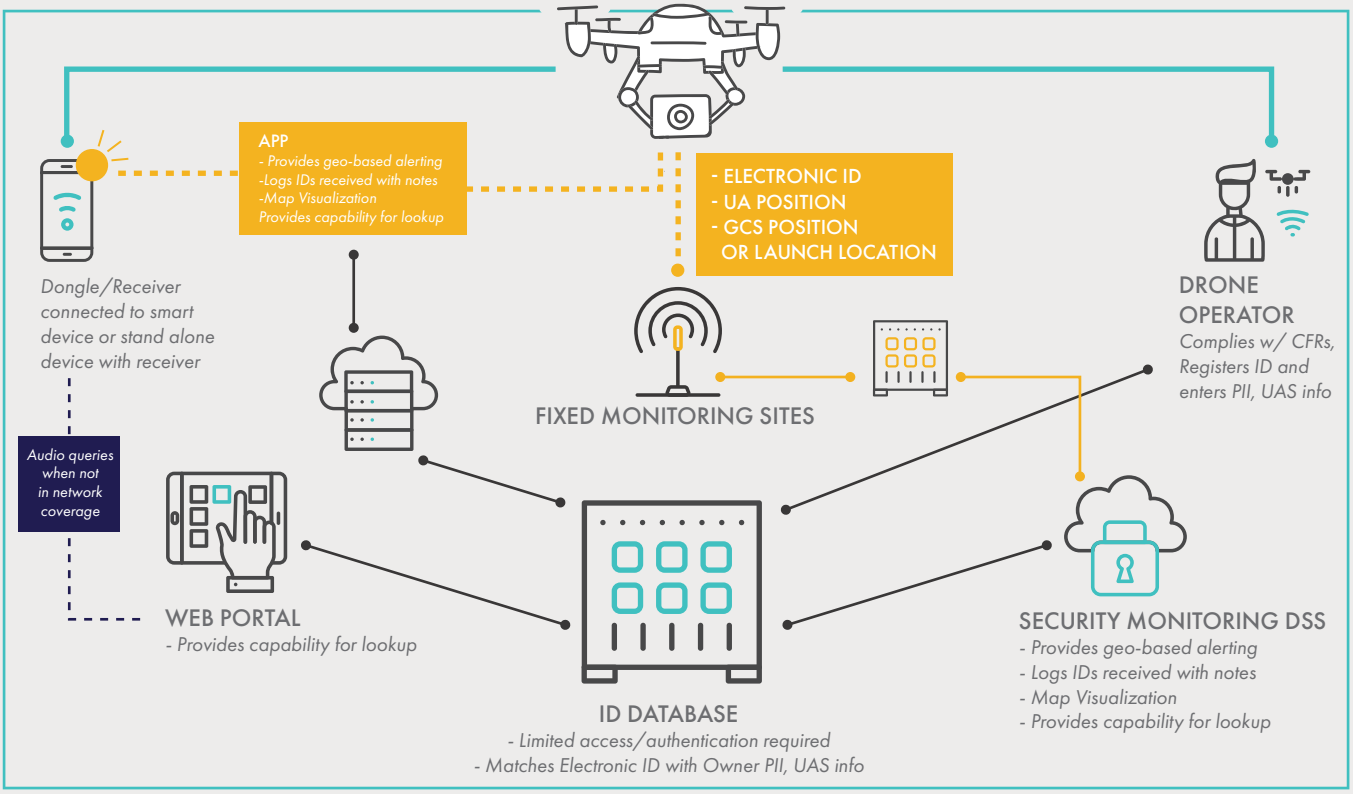


Figure 2. High Level Overview of ADS-B Architecture. (Recreation of 2017 FAA UAS ID ARC Report diagram [3])

With different vested members of industry pushing for their preferred solution(s), it is a good idea to look at them as a trade space since no one solution is a clear winner under all circumstances. Note that these values are relative

Good:
Ok:
Poor:

and entirely from the perspective of Hidden Level, Inc. There are also several that carry implied operational assumptions.

Remote ID Solutions Trade Table

	CELL	SAT	SWFN	ADSB	LPRF	UIC2	PHYS	VLE
Internet	Poor	Poor	Poor	Good	Good	Good	Good	Good
Line of Sight	Good	Good	Ok	Poor	Poor	Poor	Poor	Poor
Range	Good	Good	Ok	Ok	Poor	Poor	Poor	Poor
Altitude	Poor	Good	Ok	Good	Ok	Ok	Poor	Poor
Security	Good	Good	Ok	Poor	Poor	Ok	Ok	Ok
UAS SWaP	Poor	Poor	Ok	Good	Ok	Good	Good	Ok
Maturity	Good	Ok	Ok	Good	Ok	Poor	Good	Poor
NRE	Ok	Ok	Ok	Good	Ok	Poor	Good	Poor
Probability of Detection / False Alarm	Good	Good	Good	Good	Ok	Ok	Poor	Ok
Accuracy	Good	Good	Good	Good	Good	Good	Poor	Ok
Update Rate	Good	Poor	Good	Good	Good	Ok	Poor	Ok
Density	Good	Ok	Ok	Ok	Ok	Ok	Good	Poor
Cost	Ok	Poor	Ok	Ok	Good	Good	Good	Poor
Scale	Good	Ok	Ok	Ok	Poor	Ok	Poor	Poor
Good	9	6	3	8	4	4	6	1
Ok	2	4	10	4	6	6	1	5
Poor	3	4	1	2	4	4	7	8

A few notes about the above table:

— The "Altitude" for cellular (CELL) is rated poor since the towers are height limited and mostly point down. Future optimizations made with LTE and 5G for UAS use cases will take time so this rating is kept low for now.

— For impact to "UAS SWaP", ADS-B was rated "good". It would be a poor rating if left at the standard required power levels (i.e. from 75 to 125W)[16], however if a low power variant were allowed the SWaP impact would be minimal.[13] Lower power ADS-B also supports a higher aircraft density as described in a study done by MITRE[17]. There are also efforts to make use of protected spectrum without interfering with current ADS-B frequencies to deliver an "ADS-B like" solution that shows promise for the UAS use case [23].

— The physical indicator (PHYS) category does not readily support the "remote" part of Remote ID nor does it allow real time location reporting. It is included in the table for completeness since it was in the ARC final report [3].

A few notes about the above table *cont.*

- While visual light encoding (VLE) looks like a poor solution, there may be situations where it is acceptable and sufficient. As a universal Remote ID solution, it does not scale well.
- The "Cost" rating tries to account for total system cost including special receivers required on the UAS and/or on the ground. There may also be recurring costs (e.g. CELL subscription) that impede operator adoption. For SWFN, it is assumed the cost of the UAS link to its GCS is significant for longer range flights, but may be minimal for VLOS operations.
- Appendix B in the ARC final report[3] has an excellent trade table of similar and other attributes for consideration. The above table is mostly in agreement.
- Low Power RF (LPRF) is the proposed Broadcast solution from the ASTM F38 Remote ID and Tracking Standard[47], in the form of Wi-Fi and Bluetooth. This faces challenges in terms of its ability to function at Range, Altitude, and provide security amongst the crowded ISM band. However, it offers the ability to use ubiquitous consumer technologies at a sensible cost to the user.

From this table we can see two of the options look good: cellular and ADS-B. This assumes equal weighting of these criteria, which may not be true for each use case. For example, absent cellular infrastructure in a more remote location, ADS-B would be the only choice. But for a secure, hard to spoof link, cellular would be the clear winner. This brings us to an important point: *no one solution is ideal under all circumstances.*

Any one of these solutions, and several others being developed, may be perfectly viable for providing Remote ID. The best path forward is to define performance-based requirements for the Remote ID solution to facilitate further innovation. As UAS activity is enabled and operations increase in cadence, there will be further needs imposed on Remote ID such as longer range, higher altitudes, more security, support for increased density, higher bandwidth, etc. This will be discussed later in the section "Performance and Risk Based Requirements".

Gaps in Remote ID

With the main goals of Remote ID being full UAS cooperation, accountability, and situational awareness for safety personnel, gaps remain to give focus to. This section addresses some of these gaps, and assumes that Remote ID has been mandated, deployed, and widely used. The gaps covered below are:

1. Non-cooperative UAS
2. Position Validation
3. ID Security
4. BVLOS and Cockpit Awareness
5. Coverage and Flexibility

GAP: NON-COOPERATIVE UAS

There is a strong need to solve the security issues around airports, critical infrastructure, over people, etc., and Remote ID is seen as a means to that end. If all UAS self reported their ID and position, the airspace will be safe enough and these security issues are resolved, right? Well, sort of.

This would absolutely be true but for the reality of non-cooperative UAS; the UAS not complying with regulations supporting safe flight. The "good actors", i.e. the trained commercial UAS pilots that already know and follow the rules for safe operations, are not the actual problem. They will comply with Remote ID, nontheless potential issues around airports would remain. Even with Remote ID in full effect, non-cooperative UAS will still exist and cause unsafe conditions for manned aircraft, other UAS, and bystanders.

Gap: Non-cooperative UAS *Cont.*

In this context a non-cooperative UAS could be any one of the following:

- UAS operators unaware Remote ID is required
- Operators with legacy UAS that either do not want to upgrade to support Remote ID due to cost, SWaP, etc. or have a UAS that cannot be retrofit
- Operators believing they fly safe enough without Remote ID
- Operators refusing to share personal information if not otherwise doing anything wrong
- Bad actors purposely disguising or hiding their activity

Education will continue seeking to reduce or eliminate the "clueless" operators. Mandatory Remote ID will bolster law enforcement capability to enforce compliance and UAS operators found not complying will be held accountable. Even with a raised sense of accountability, the increasing availability of low cost UAS and a growing number of potentially uneducated operators will challenge compliance in the near term.

The number of legacy UAS, reported to be in the hundreds of thousands[18], presents a big issue for Remote ID compliance. Consideration has been given in the past[3] and continues to be evaluated[47] when determining viable Remote ID solutions based on how easy they are to retrofit to existing UAS. However, this may not be feasible for all legacy UAS causing the inevitability of operators who will continue to operate without Remote ID.

Alternative ways to provide Remote ID data in safety critical settings even for *non-cooperative* UAS are needed. Technologies that can supplement the data provided by Remote ID compliant UAS with non-participant UAS data can help fortify the safety of the low altitude airspace ecosystem.

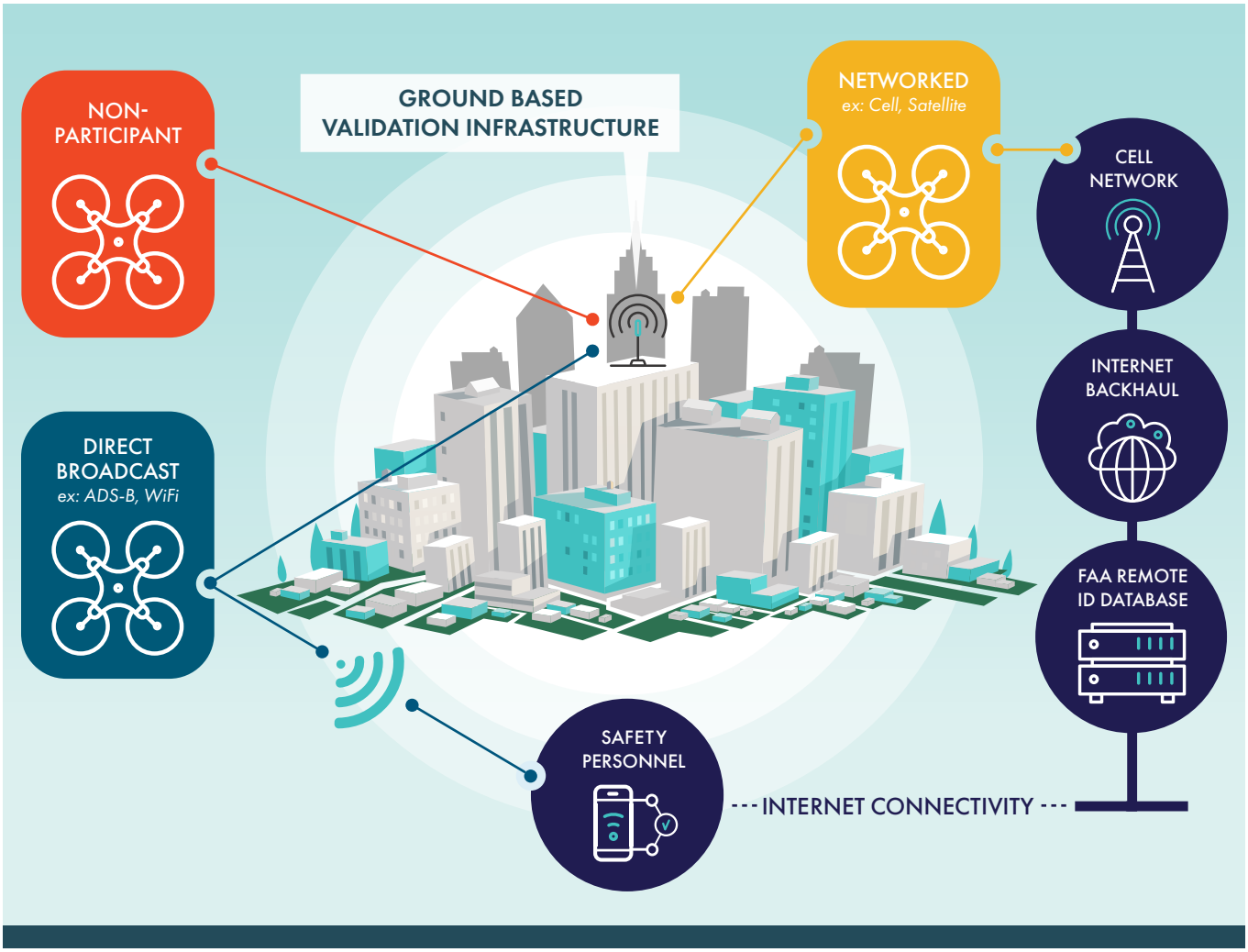


Figure 3. Ground Based Validation Infrastructure Supporting Remote ID Ecosystem

GAP: POSITION VALIDATION

Even if all UAS employed Remote ID, there is still the question of "has the reported position been verified, can it be trusted?" Additionally, there may be legitimate cases where even a certified UAS reported position may not satisfy required accuracy in terms of position, velocity, and/or altitude. This can happen for several reasons, some of which are particular to smaller UAS operations at low altitudes[20]:

The onboard GPS is erroneous from a lack of line of sight to enough satellites, possibly due to the platform roll-pitch-yaw and/or nearby buildings, trees, or other obstructions

The onboard GPS experiences multi-path or excessive fading in an urban canyon

The onboard IMU/INU is momentarily affected by interference

Positional anomalies are often mitigated by having two or more redundant GPS devices on the UAS, or some other auxiliary method of determining geolocation. However, nothing is guaranteed and there are cases where the UAS may knowingly declare a degraded state along with its reported position, or unknowingly be in one. In either case, safety of the airspace is compromised.

This is a known issue in manned aviation and for ADS-B, which is a key component of the NextGen system[21]. Systems have been put in place near critical areas to "validate" the ADS-B position with a secondary source. This is done in real time and at any point the reported position can be validated or invalidated. Additional work has been done in RTCA SC-228 on the DAA MOPS (DO-365) with regards to ADS-B validation[22] to ensure that larger UAS are reporting an accurate position needed for conflict resolution.

In the near term, UAS Remote ID may not need position validation; for example if flights are done in remote locations and away from critical infrastructure, airports, and other areas of concern. Long term, as the number and frequency of UAS operations increase, when and how can the Remote ID position be validated? A corollary to the solution in place for commercial ADS-B validation with ground based infrastructure could help improve the safety assurances of low altitude UAS operations for critical areas.

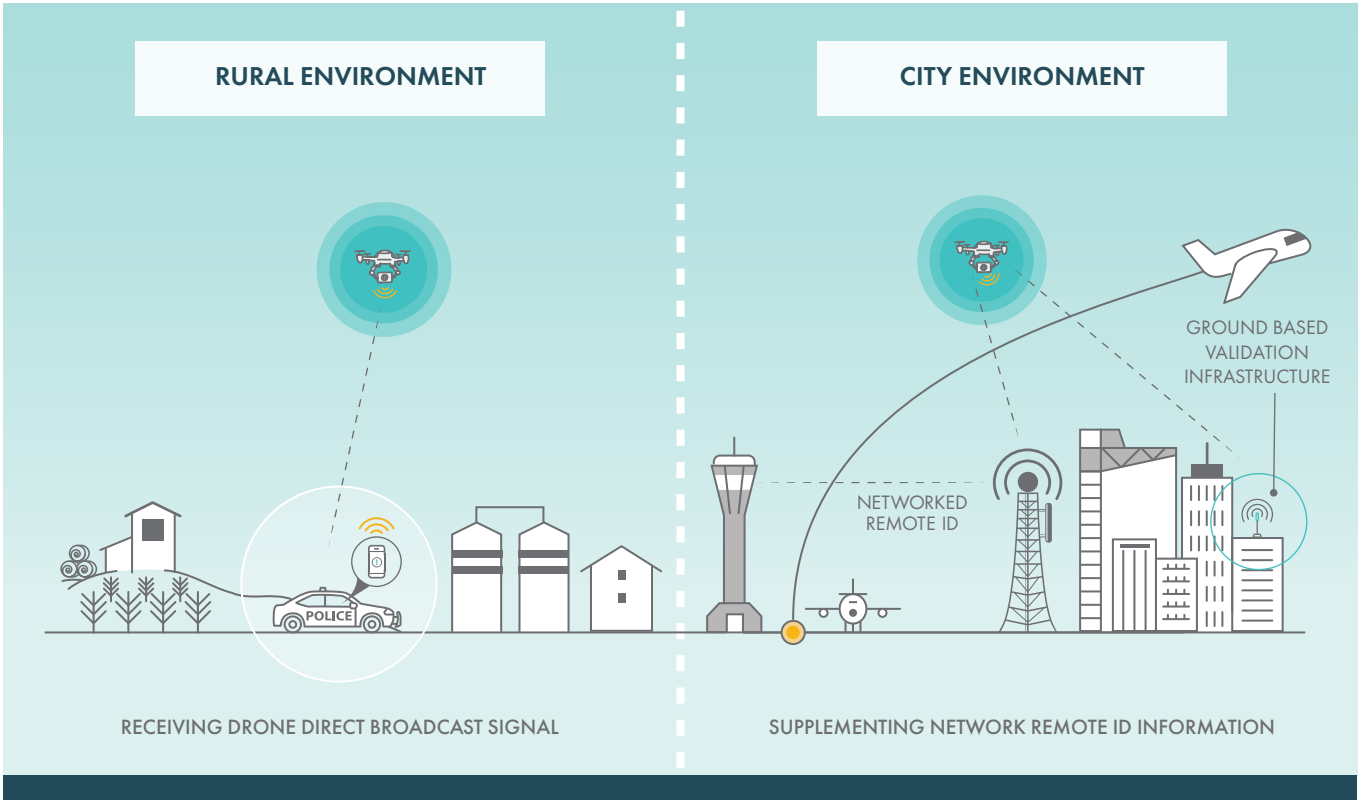


Figure 4. Contrasting Remote ID Operational Environment Needs

GAP: DATA SECURITY

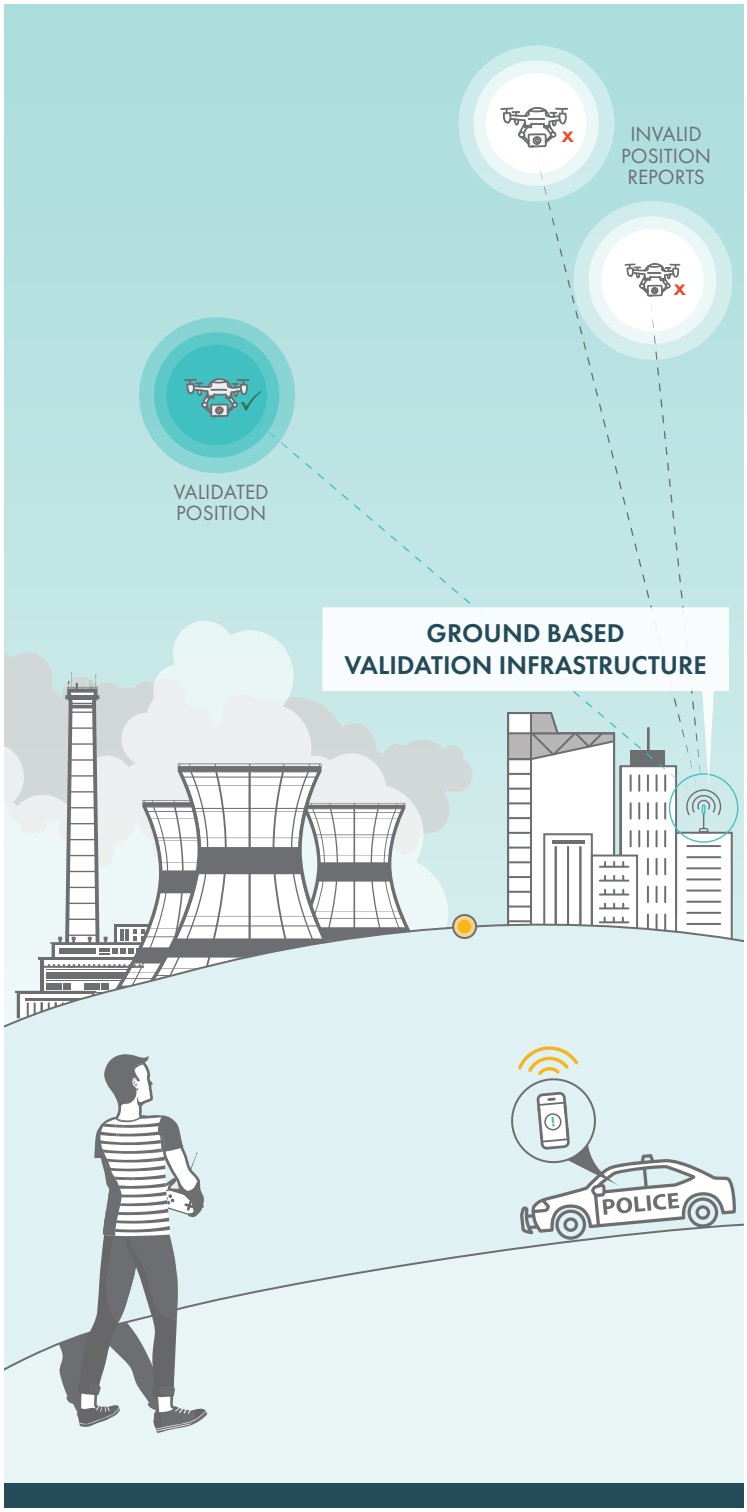


Figure 5. Validating Remote ID Positional Reports For Critical Airspace

To ensure the safety of the NAS and provide effective avenues to enforcement, it is important to have secure, trustworthy Remote ID. Some of the near term solutions (e.g. cellular) are fairly secure under most circumstances, especially coupled with underlying network authentication, while some broadcast solutions can be readily spoofed (e.g. ADS-B) [24]. For the near term need to roll out Remote ID, this is probably not a big issue. For example, ADS-B has been in use for manned aircraft for quite some time and while there are countless articles pointing out the security flaws it has, there are no reported cases of someone spoofing a commercial aircraft for nefarious reasons even though it has been possible with COTS electronics for about 20 years now[30]. Solutions like ADS-B remain viable for low altitude Remote ID, but bring with it the concern of data security.

For the long term, it is worth thinking about solutions for Remote ID security regardless of the near term solutions used. Many good ideas have been proposed for this [31][32][33]. Additionally, the Remote ID Position Validation gap solution mentioned earlier can also function as a future security measure by checking that the reported Remote ID position is indeed where it claims to be. If the RF signal being used for Remote ID can be detected and correlated with the reported position, not only will the information be validated for accuracy, but it will have been inadvertently checked for spoofing as well. Validation could be done with more than one verification method as dictated by the operational environment, for example close to a major airport. This is in fact how the FAA validates ADS-B for both accuracy and legitimacy near the largest airports; using a combination of multilateration, secondary surveillance, and primary surveillance. UAS Remote ID security can be built up in a similar fashion as needed to enable more operations in higher risk areas.

GAP: BVLOS AND COCKPIT AWARENESS

The FAA has stated that Remote ID is a critical step towards enabling Beyond Visual Line of Sight (BVLOS) operations[25] and this has been echoed by others. However, Remote ID alone does not solve the main challenge for BVLOS; the ability to see and avoid another aircraft as dictated in 91.113[28]. There are more than 200,000 active general aviation (GA) aircraft in operation within the United States alone[29], many of which fly without an active transponder in class G airspace, and some even fail to use transponders in controlled airspace. Even if UAS are reporting their own position in real time and able to avoid each other, how will the UAS avoid the manned aircraft and vice versa?

In general the UAS cannot "see" GA aircraft, nor can the GA aircraft visually see the smaller UAS.

One proposed solution that has been put forth is specific to controlled airspace. Given the FAA Jan 2020 mandate for ADS-B Out equipage[26] as part of its Next Gen initiative, most all aircraft will be broadcasting their location in controlled airspace, including GA aircraft. If UAS could ingest this data real time then they could give the manned aircraft right of way and avoid them safely. In other words, UAS could electronically "see" the manned aircraft. Some manufacturers are proposing this as a universal capability for their future designs[27] and some vendors have low SWaP ADS-B In devices available[34]. This is an excellent step in the right direction and will increase awareness and safety. However it does not solve the general case of needing to avoid manned aircraft at low altitudes and in all classes of airspace, including where BVLOS UAS operations are desired (e.g. remote pipeline inspections[38]). Additionally, there will still be some manned aircraft that are exempt from or fail to adhere to the ADS-B Out rule, for example hot air balloons, gliders, and other vehicles lacking electrical systems. UAS may be able to detect these with onboard sensors and/or with procedures to avoid known activity, but will it be enough?

Flipping the problem around, the manned aircraft could ingest the UAS Remote ID information for situational awareness or at least to avoid the initial UAS BVLOS operational areas. This is referred to as "cockpit awareness" and may be accomplished via checks of UAS targets both pre-flight and in flight operation displayed on existing systems. A recent white paper on this topic[35] gives several examples of how this could be accomplished through the use of well-established procedures and existing equipment in use today.

Unfortunately, this particular gap in Remote ID will not be solved without some additional effort.

Primary radar is the go-to solution to "see everything" in the sky, but is expensive to buy, deploy, and maintain and has target classification, false alarm reporting, range, and low altitude accuracy issues. This applies to ground-based as well as airborne radar. Plenty of worthwhile testing and development is being done in these areas but there is no clear solution yet.

Stereoscopic optical sensors show promise as well, even if they may be limited to clear visibility conditions for now. If the issue of slower non-cooperative aircraft (e.g. hot air balloons) can be addressed using optics, it will go a long way as part of the larger solution[42][43].

As explained above, the dream of a "fully cooperative" sky may be a ways off, even with Remote ID fully deployed and the ADS-B Out rule in effect. It is worth planning for, but for the next few years Remote ID will need augmentation for UAS operations that need to take place in or near high risk areas, such as near airports, over people, near critical infrastructure, etc.

GAP: COVERAGE AND FLEXIBILITY

The last gap for Remote ID is in coverage and flexibility. Regardless of the solution(s) chosen to satisfy performance needed, there will always be a desire for long range, ubiquitous coverage for the entire airspace. There will be cases when short-range direct broadcast will be insufficient, and there will be cases when networked solutions (e.g. cellular and/or internet) will be lacking. Consider UAS operations during disaster relief efforts facing little to no network connectivity due to the results of the disaster itself or the location being a remote area without connectivity infrastructure. There have been several cases[44][45] where UAS flights from non-cooperatives were interfering with the air boss and other safety personnel missions which could involve a vast operational area.

Even with industry-wide Remote ID adoption and implementation, there may be need for mobile solutions to cover some of these edge cases. Having semi-permanent infrastructure that can be moved and setup in hours and left for weeks on end would mitigate this gap.

This mobile infrastructure could also act as a command and control link boost extending the capability of friendly UAS in the area. The mobile infrastructure's ability to provide airspace assurance or at least add some desired redundancy for dangerous and difficult operating environments is a valuable risk mitigation.

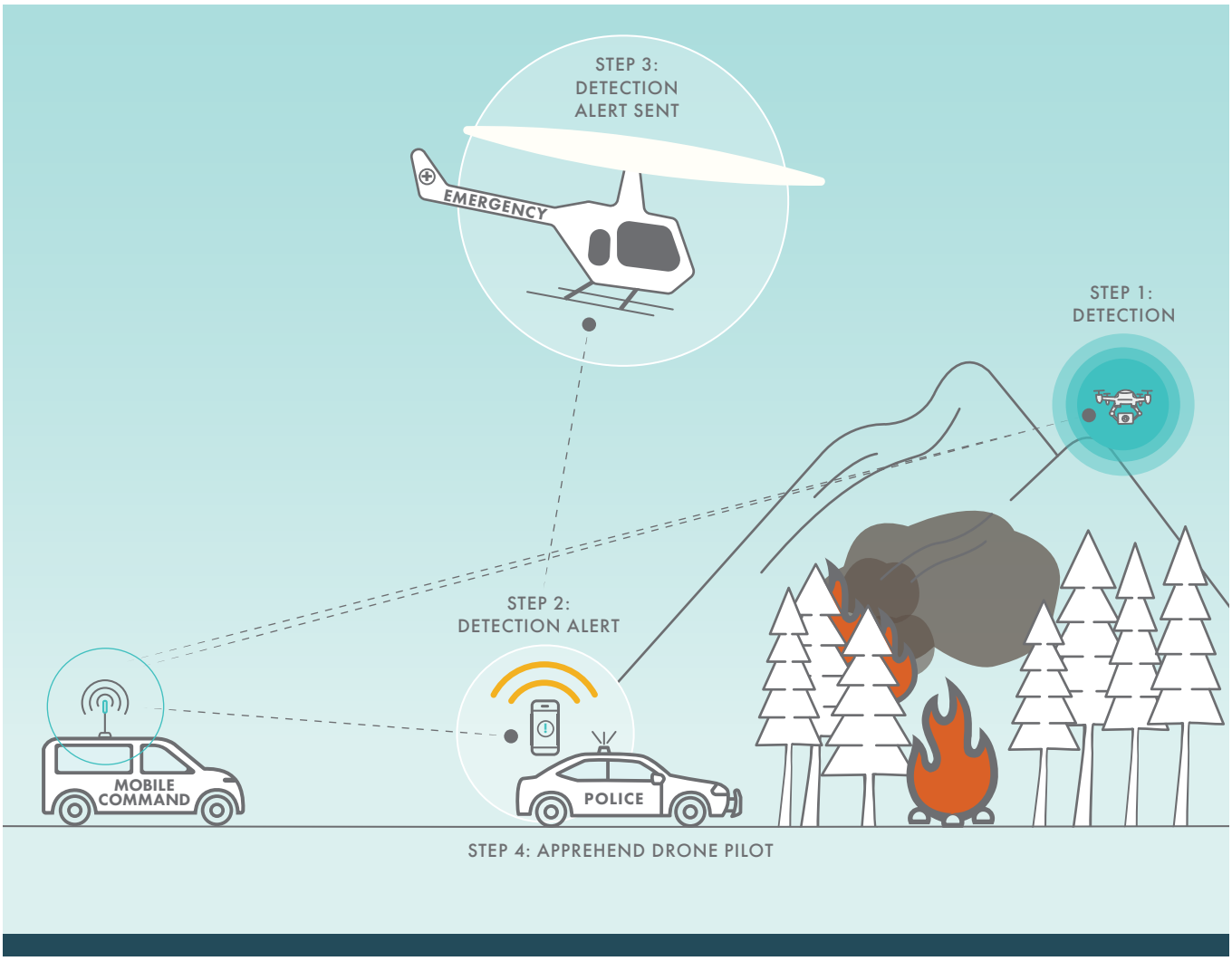


Figure 6. Mobile Deployment Supporting Remote ID In Dynamic Operational Environment

Performance and Risk Based Requirements

After identifying some of the long term gaps associated with Remote ID, we turn our attention back to the near term needs. As previously highlighted, there are several solutions for Remote ID available today that will go a long way to making the airspace safer. The missing component to all of this is some line in the sand in the form of initial performance-based requirements.

It would not be difficult to establish initial performance-based specifications with all the previous subject matter expertise available, both from the UAS community as well as the last 50+ years of aviation history. Some requirements were proposed in table 3 and within the ARC's final report[3], which are integrated alongside initial suggestions of our own. These requirements should not be considered final of course, and also may need an operational environment constraint imposed, for example far enough from airports, critical infrastructure, densely populated areas, etc. These are meant to be a starting point, aimed at a common concept of operation (e.g. Law Enforcement) that need to have a display showing UAS activity within some limited area of interest.

#	REQUIREMENT	VALUE	DESCRIPTION
1	Range	≥ 1 km	This is the broadcast range from the UAV of interest to the receiver device consuming the Remote ID data, longer range preferred.
2	Altitude	≥ 500 meters (AGL)	While a UAV may not normally be flying this high, it is important to have a Remote ID solution that can provide a sufficient situational awareness buffer.
3	Update Rate	≥ 0.5 Hz	Enough update rate to provide a clear visual indicator of the UAV activity.
4	Latency	≤ 3.5 seconds	Minimal latency needed to provide actionable data (i.e. reaction time).
5	Accuracy	≤ 50 meters (SEP)	50% Spherical Error Probable needed to provide accurate actionable data. Note this is spherical to include elevation/height.
6	Ptrk	≥ 95%	Probability of track establishment (continuous location updates).
7	Pfa	≤ 1/hour	Probability of false alarm (track). Need to keep as low as possible to avoid alert fatigue.
8	Density	≥ 1 UAV per 0.5 km^2	This is the minimum density the Remote ID solution should support.
9	Uptime	≥ 99%	The Remote ID solution must be reliable enough to be usable.

These can be considered "minimal operational performance specifications" (MOPS) since more implementation specific requirements are left out. The implementation requirements are likely to be more thoroughly covered by the initial release of the ASTM Remote ID and Tracking Standard[47]. With some performance specifications proposed, we can now turn our attention to the next step: testing and data collection.

TESTING AND DATA COLLECTION

To avoid the "analysis paralysis" that can occur with defining "safe enough", it is critical to begin formalized testing and data collection on the various Remote ID solutions to help shape and inform the final requirements. There are many ways to go about this, and they all involve industry participation. The approach taken by the NASA UTM[41] project and its Technical Capability Level (TCL) testing is a model worth emulating to achieve critical data points supported by industry participation. In the United States, the FAA must answer the question of what is "good enough" with data and due diligence supporting ensured safety of the National Airspace System.

Any vendor or vested party with one or more Remote ID solutions can begin collecting data against these initial performance requirements and show where they stand. Working with groups such as ASTM F38[47] is a good idea, especially for furthering performance specifications, and partnering with any one of the FAA's extended parties will provide even more legitimacy. Within the United States this would include one or more FAA test sites[39], the Center of Excellence (ASSURE)[40], NASA[41], and so on. Hidden Level is committed to helping the aviation industry take the next step with Remote ID technology and calls to other industry contributors to continue building requirements through testing and data collection efforts.

RISK BASED REQUIREMENTS

According to the US Department of Transportation, Remote ID is intended to "address security and law enforcement concerns regarding the further integration of these aircraft into the national airspace while also enabling greater operational capabilities by these same aircraft"[46]. Many in the UAS Industry are hopeful in taking this vision statement forward into a multi-phase effort in which the usage of Remote ID will evolve into a supporting piece of advanced BVLOS operations. In order to reach support of these advanced operations, risk based requirements must be established along each advanced step.

At its core, Remote ID helps give transparency to drone operations, certainly initially to help law enforcement easily distinguish intent of drones participating cooperatively in the airspace. The common tracking and identification information provided by Remote ID can also support a more accurate characterization of airspace operations, once initially deployed/adopted, that can inform thoughtful rulemaking for public and commercial drone operations. The capability and assurance of Remote ID transmitted information can be used to support adoption of Risk Based Requirements to address operations in different volumes of airspace.

RISK LEVEL	AIRSPACE CHARACTERISTICS	EXAMPLE USE CASES	RISK BASED CONSIDERATIONS
Low	— Rural/Remote — Limited/No Network Access — Low Probability of Dense Aircraft Operations or Encountering Non-Cooperatives	— Linear Infrastructure Inspection — Precision Agriculture — Long Haul BVLOS Operations	— Direct Broadcast Required — Utilize Network when accessible — Little to no need for redundancy, positional validation — Class G airspace transponder requirements
Medium	— Suburban/Urban — Network Access — Cooperative and Non-cooperative Aircraft Operations Present	— Repeatable/routine operations — Disaster Response	— Augment Network connectivity with Direct Broadcast — Supplemental information from ground-based validation infrastructure, where available
High	— Dense Urban — High Fidelity Network Access — High Probability of Cooperative and Non-cooperative Aircraft Operations	— Operations Over People — Operations Near/Over Critical Infrastructure	— Network can display full airspace picture, augmented by ground based infrastructure Direct Broadcast receipts — Need for redundancy, positional validation, anti-spoofing assurances from ground-based validation infrastructure — Additional capabilities such as spectrum monitoring and backup C2 provisions

Using the high level outline of Remote ID scenarios from the table above, it reinforces the "walk before you run" approach by first integrating Remote ID and verifying its enabling capability with low-risk environments. In order to build a compelling safety case for integration of Remote ID moving from the lower to higher risk scenarios, performance standards and requirements for supporting ground-based infrastructure must be put in place to mitigate potential risks and provide the data-driven due dilligence to support safe integration of UAS into the NAS.

Conclusion and Next Steps

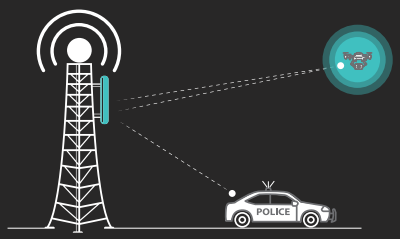
This white paper has made an effort to enforce the following takeaways:

1

Initial performance-based requirements should be established for Remote ID. They do not have to be perfect or final, but subject matter experts could make fairly good guesses at what would be sufficient to get airborne.

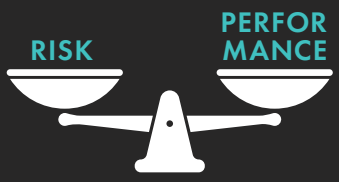
2

Several viable solutions for Remote ID exist today and should be employed immediately, even if under certain constraints (ex: limited operational environments)



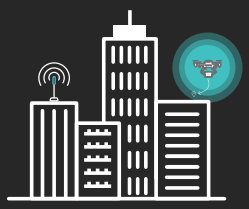
3

Thorough testing and data gathering can vet out these solutions quickly, over months not years, and inform the necessary performance and risk based requirements for Remote ID



4

Longer term solutions, such as ground-based infrastructure, for Remote ID can help fill the gaps of these implementations, build upon the present requirements, and allow UAS operations in higher risk areas by adding improved performance, reliability, security, and coverage.



Appendix

REFERENCES

[1] FAA (2018-07-30), "Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap": https://www.faa.gov/uas/resources/policy_library/media/Second_Edition_Integration_of_Civil_UAS_NAS_Roadmap_July%202018.pdf

[2] FAA (Last Updated 2019-07-22), "UAS Data Exchange (LAANC)": https://www.faa.gov/uas/programs_partnerships/data_exchange/

[3] FAA (2017-09-30), "UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee (ARC), ARC Recommendations Final Report": https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS%20ID%20ARC%20Final%20Report%20with%20Appendices.pdf

[4] FAA (Last Updated 2019-07-11), "Register Your Drone": https://www.faa.gov/uas/getting_started/register_drone/

[5] FAA (2015-12-14), "Press Release - FAA Announces Small UAS Registration Rule": https://www.faa.gov/news/press_releases/news_story.cfm?newsId=19856

[6] Minnesota DOT (2019-07-26), "Improving the Quality of Bridge Inspections Using Unmanned Aircraft Systems (UAS)": https://www.dot.state.mn.us/research/reports/2018/201826.pdf

[7] DJI (2019-07-26), "Fly Safe with DJI": https://www.dji.com/flysafe

[8] FAA (2019-07-26), "Know Before You Fly": http://knowbeforeyoufly.org/

[9] NASA (2019-09-04), "UAS Traffic Management (UTM) Project": https://www.nasa.gov/aeroresearch/programs/aosp/utm-project-description/

[10] Electronic Code of Federal Regulations (2019-08-02), "Part 107 - Small Unmanned Aircraft Systems": https://www.ecfr.gov/cgi-bin/text-idx?SID=fb017ad749ab71723a55698dd383ca65&mc=true&node=pt14.2.107&rgn=div5

[11] FAA (2019-02-26), "Certificated Remote Pilots including Commercial Operators": https://www.faa.gov/uas/commercial_operators/

[12] FAA (2019-07-22), "UAS Data Exchange": https://www.faa.gov/uas/programs_partnerships/data_exchange/

[13] uAvionix (2017-03-22), "Concepts for Remote Identification": https://uavionix.com/downloads/whitepapers/uavionix-remote-identification-white-paper.pdf

[14] WhiteFox Defense Technologies (2019-05-30), "Enabling the Good While Preventing the Bad: How Security Enables the Drone Industry": https://docsend.com/view/rih9yhk

[15] Kittyhawk (2019-03-12), "Remote ID & Commercial Drones": https://kittyhawk.io/resources/Remote-ID-White-Paper.pdf?dl=1

[16] RTCA (2011-12-13), "Minimum Operational Performance Standards for 1090 MHz Extended Squatter Automatic Dependent Surveillance – Broadcast (ADS-B) and Traffic Information Services – Broadcast (TIS-B)": https://standards.globalspec.com/std/1994503/RTCA%20DO-260

[17] MITRE (2017-01-05), "ADS-B Surveillance System Performance with Small UAS at Low Altitudes": https://www.mitre.org/sites/default/files/publications/16-4497-AIAA-2017-ADS-B.pdf

[18] FAA (2019-07-12), "Unmanned Aircraft Systems": https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/Unmanned_Aircraft_Systems.pdf

[19] Wikipedia (Last Updated 2019-08-12), "Gatwick Airport drone incident": https://en.wikipedia.org/wiki/Gatwick_Airport_drone_incident

[20] American Institute of Aeronautics and Astronautics (2017-06-09), "Hazards Identification and Analysis for Unmanned Aircraft System Operations": https://utm.arc.nasa.gov/docs/2017-Belcastro_Aviation_2017-3269_ATIO.pdf

[21] FAA (Last Updated 2019-06-25), "NextGen": https://www.faa.gov/nextgen/

[22] RTCA (Last Updated 2019-03-01), "SC-228, Minimum Performance Standards for Unmanned Aircraft Systems": https://www.rtca.org/content/sc-228

[23] uAvionix (2019-10-07), "uAvionix Receives an DAA Transmission License to Test UDS-B Solution": https://uavionix.com/uavionix-test-uds-b-solution/

[24] Government Accountability Office (2018-01-18), "Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft": https://www.gao.gov/products/GAO-18-177

[25] FAA (2018), "Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap": https://www.faa.gov/uas/resources/policy_library/media/Second_Edition_Integration_of_Civil_UAS_NAS_Roadmap_July%202018.pdf

[26] FAA (Last Updated 2019-08-06), "Equip ADS-B": https://www.faa.gov/nextgen/equipadsb/

[27] DJI (2019), "DJI AirSense": https://www.dji.com/flysafe/airsense

[28] Electronic Code of Federal Regulations (2019), "Right-of-way rules: Except water operations": https://ecfr.io/Title-14/pt14.2.91#se14.2.91_1113

[29] FAA (2019-06-01), "Air Traffic By The Numbers": https://www.faa.gov/air_traffic/by_the_numbers/media/Air_Traffic_by_the_Numbers_2019.pdf

[30] Andrei Costin, Aurelien Francillon, EURECOM (2012), "Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices": https://media.blackhat.com/bh-us-12/Briefings/Costin/BH_US_12_Costin_Ghosts_In_Air_WP.pdf

[31] Sudhindra Nayak (2018-12-06), "A Cryptographic Proof-of-Concept for Securing Aircraft ADS-B Data": https://www.eeweb.com/profile/sudhindra-nayak/articles/a-cryptographic-proof-of-concept-for-securing-aircraft-ads-b-data

[32] Richard C. Agbeyibor (2014-03-01), "Secure ADS-B: Towards Airborne Communication Security In The Federal Aviation Administration's Next Generation Air Transportation System": https://apps.dtic.mil/dtic/tr/fulltext/u2/a600893.pdf

[33] Emily Cook (2015-08-24), "ADS-B, Friend or Foe: ADS-B Message Authentication for NextGen Aircraft": https://ieeexplore.ieee.org/document/7336340

[34] uAvionix (2019), "Products": https://uavionix.com/products/

[35] Aviators Code Initiative (2019-03-08), "Improving Cockpit Awareness of Unmanned Aircraft Systems Near Airports": http://www.secureav.com/UAS-Awareness-WP-v1.0.pdf

[36] FAA (2013), "FAA Aerospace Forecast Fiscal Years 2013- 2033": https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/2013_forecast.pdf

[37] FAA (2019), "FAA Aerospace Forecast Fiscal Years 2019-2039": https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/FY2019-39_FAA_Aerospace_Forecast.pdf

[38] Miriam McNabb (2019-08-02), "Inside the First Truly BVLOS Quadcopter Drone FlightWithout Ground Observers": https://dronelife.com/2019/08/02/inside-the-first-truly-bvlos-drone-flight-without-ground-observers-a-4-mile-linear-inspection-along-the-trans-alask-pipeline/

[39] FAA (2018-10-23), "UAS Test Sites": https://www.faa.gov/uas/programs_partnerships/test_sites/

[40] ASSURE (2019), "The FAA's Center of Excellence for UAS Research Alliance for System Safety of UAS through Research Excellence": http://www.assureuas.org/about.php

[41] NASA (2019), "UAS Traffic Management (UTM) Project": https://www.nasa.gov/aeroresearch/programs/aosp/utm

[42] Robotics Business Review (2019-08-02), "Alaska Team Performs BVLOS Drone Flight Without Human Observers": https://www.roboticsbusinessreview.com/unmanned/unmanned-aerial/alaska-team-performs-bvlos-drone-flight-without-human-observers/

[43] Haye Kesteloo (2019-03-20), "How the autonomous Skydio R1 drone views the world as it is following you": https://dronedj.com/2018/03/20/how-the-autonomous-skydio-r1-drone-views-the-world-as-it-is-following-you/

[44] Kristen Inbody (2018-08-13), "Drones interfering with wildland firefighting across the West": https://www.greatfallstribune.com/story/news/2018/08/13/drones-interfering-firefighting-fires-across-west-montana/980301002/

[45] Melissa Quinn (2017-09-09), "Harvey forces debate over using drones in disaster recovery": https://www.washingtonexaminer.com/harvey-forces-debate-over-using-drones-in-disaster-recovery

[46] U.S. Department of Transportation (2019-09-06), "Report on DOT Significant Rulemakings": https://www.transportation.gov/sites/dot.gov/files/docs/regulations/350431/august-2019-significant-rulemaking-reportfinal.docx

[47] ASTM International (2019), "Standard Specification for Remote ID and Tracking": https://www.astm.org/DATABASE.CART/WORKITEMS/WK65041.htm